




RESEARCH ARTICLE

Cybersecurity risk assessment of VDR

Ömer Söner,^{1*}  Gizem Kayisoglu,² Pelin Bolat,³ and Kimberly Tam⁴

¹ Department of Maritime Transportation Management Engineering in Maritime Faculty, Van Yuzuncu Yıl University, Van, Türkiye

² Department of Maritime Transportation Management Engineering in Maritime Faculty, Istanbul Technical University, Istanbul, Türkiye

³ Department of Basic Sciences in Maritime Faculty, Istanbul Technical University, Istanbul, Türkiye

⁴ School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth, UK.

*Corresponding author. E-mail: soneromer023@gmail.com

Received: 28 May 2022; **Accepted:** 8 October 2022; **First published online:** 31 January 2023

Keywords: maritime; cybersecurity; risk assessment; VDR; FMEA

Abstract

The voyage data recorder (VDR) is a data recording system that aims to provide all navigational, positional, communicational, sensor, control and command information for data-driven investigation of accidents onboard ships. Due to the increasing dependence on interconnected networks, cybersecurity threats are one of the most severe issues and critical problems when it comes to safeguarding sensitive information and assets. Cybersecurity issues are extremely important for the VDR, considering that modern VDRs may have internet connections for data transfer, network links to the ship's critical systems and the capacity to record potentially sensitive data. Thus, this research adopted failure modes and effects analysis (FMEA) to perform a cybersecurity risk assessment of a VDR in order to identify cyber vulnerabilities and specific cyberattacks that might be launched against the VDR. The findings of the study indicate certain cyberattacks (false information, command injection, viruses) as well as specific VDR components (data acquisition unit (DAU), remote access, playback software) that required special attention. Accordingly, preventative and control measures to improve VDR cybersecurity have been discussed in detail. This research makes a contribution significantly to the improvement of ship safety management systems, particularly in terms of cybersecurity.

1. Introduction

The voyage data recorder (VDR) is one of the most critical systems onboard ships that can preserve crucial information about a ship to enable a data-driven investigation to identify the cause(s) of ship accidents. Therefore, it is dangerous if access to its data is limited, or is poorly recorded (OCIMF, 2020). VDR requirements have recently been revised due to new improvements in information and communications technology (ICT). This enables shipowners, operators and accident investigators to access all pertinent information. With this amendment, new VDRs have to meet expanded requirements, such as recording data for longer periods of time, as well as providing additional data input sources (IMO, 2012). Moreover, new VDRs may provide remote connectivity to transfer large amounts of data.

Big Data and the Internet of Things (IoT) are being rapidly adopted by the shipping industry to transform many aspects of shipping operations, not only for safety-critical applications and data-driven decision making, but also for real-time monitoring and reducing pollution. New VDR regulations may enhance safe navigation and optimisation, given the large range of ship operating data (Barkow et al., 2011; Danelec, 2021). While the VDR's main purpose is to store information, for compliance with the industry regulations, remote navigational assessments and audits can provide an effective way of

navigational safety decision support, rapid analysis following an incident, and lower audit expenses or, more significantly, increase audit frequency (OCIMF, 2020). Apart from forensic analysis, proactive use of VDR data can substantially reduce the number of accidents reported by the shipping industry (Piccinelli & Gubian, 2013). Since a ship's performance optimisation requires high-dimensional ship operating data, new VDR data would be particularly beneficial when used to improve ship energy efficiency and environmental performance (Perera & Mo, 2020).

ICT has introduced new advantages for the shipping industry, and also increased the vulnerability of shipboard information technology (IT) and operational technology (OT) infrastructure to cyberattacks (Heering et al., 2021). As modern ship's systems connect to shoreside networks through the internet, new points of vulnerability emerge that cyberattackers might use to get sensitive information, disable essential equipment, steal identities, help in smuggling commodities and even hijack a ship, its crew and its cargo (Danelec, 2016; Tam and Jones, 2019). In addition to network security, which can affect a VDR, data protection and hardware security, cybersecurity is a concern with all of the dangers that intentional and unintentional cyberthreats may pose to the information systems. Therefore, cybersecurity is of paramount importance for the shipping industry.

Regarding cybersecurity, shipping stakeholders have presented new standards, requirements, resolutions, guidelines and recommendations to raise awareness of cyber risks and vulnerabilities in the shipping industry. The International Maritime Organization (IMO) has published a guideline on maritime cyber risk management (IMO, 2016), and the American Bureau of Shipping (ABS) has developed standards for marine and offshore cybersecurity (ABS, 2016). Numerous shipping organisations, such as BIMCO (Baltic and International Maritime Council), CLIA (Cruise Lines International Association) and ICS (International Chamber of Shipping), have collaborated to develop a unique cybersecurity guideline onboard ship to assist in the implementation of a competent cyber risk management plan (BIMCO, 2020).

The number of studies on cybersecurity assessment research is also growing. One main theme is cyber risk assessment for autonomous ships (Katsikas, 2017; Tam and Jones, 2018; Kim et al., 2020; Zhou et al., 2020, 2021). Another popular area of research is the security assessment of ship control systems (Babineau et al., 2012; Shang et al., 2019; Svilicic et al., 2019c; Bolbot et al., 2020; Kavallieratos and Katsikas, 2020). Complex methodological techniques have been introduced to perform cybersecurity analysis (Kavallieratos et al., 2018; Omitola et al., 2018; Glomsrud and Xie, 2019; Guzman et al., 2019). Similarly, critical ship and port operational technology systems, such as ECDIS (Electronic Chart Display and Information System) (Svilicic et al., 2019a, 2019b) and port infrastructure (Papastergiou et al., 2015; Gunes et al., 2021; Tam et al., 2021), have also been investigated. Cybersecurity risk has become a major concern for the shipping industry as a result of recent reported instances (Heering et al., 2021; Meland et al., 2021). Ships' IT and OT systems are particularly vulnerable, as they were built with relatively low awareness of cybersecurity (King, 2005). Cyberattacks can have significant outcomes. For example, three fishermen died when the Singaporean ship *Prabhu Daya* collided with a fishing boat in 2012 (MD, 2022), but when officials boarded the ship, one of the members of the officials inserted a USB stick into the VDR, causing all data to be lost. Santamarta (2015) reported that the VDR data files on an Indian cargo ship were also overwritten using a USB stick.

Despite the considerable research and worldwide effort, cyberattacks in the shipping industry are increasing at an alarming rate. Since modern VDRs may have internet connections for data transfer, network connections to the ship's critical systems (Automatic Identification System (AIS), ECDIS, etc.) and the ability to record potentially sensitive information, cybersecurity considerations are crucial (OCIMF, 2020). As the literature review reveals, research that is specifically dedicated to investigating VDR cybersecurity risk is currently lacking. Therefore, it is critical to take the required steps to safeguard VDR from current and emerging cybersecurity threats. To fill this gap, the aim of this study is to apply a quantitative risk assessment to analyse cybersecurity risk, taking into consideration industry expectations, technical changes and literature shortages, in order to remedy these aforementioned gaps. Accordingly, the objective of this study is to put forward cyber vulnerabilities and specific cyberattacks

that might be launched against the VDR via the failure modes and effects analysis (FMEA) method that allows the components, modules and subsystems of a system to be examined and the failure modes, causes and consequences of the system to be defined. The structure of the study is outlined as follows. The first section deals with the study motivation and a literature review. The second section of this study presents the utilised model. In the next part, the case study is performed. The last section concludes the study and discusses future research.

2. Methodology

FMEA is a systematic analytical technique that allows a system's probable failure modes, failure causes, failure consequences and problem areas to be identified, avoided and remedied (Stamatis, 2003). FMEA has been used as a risk assessment method to discover failure modes and prioritise them for proactive measures since it is an inductive technique (Liu, 2016). FMEA was first established as a formal design approach in the aerospace industry in the 1960s, and its use has since spread to other industries to enhance the reliability and safety of commodities, processes, systems and services (Cicek and Celik, 2013; Liu et al., 2015). FMEA cybersecurity risk assessment is viable now, as well (Ralston et al., 2007; Haseeb et al., 2021), as it investigates components, modules and subsystems to define failure modes in a system, as well as their causes and ramifications, and it may analyse the risks associated with cyber components (Akula and Salehfar, 2021).

FMEA is carried out via a sequence of steps: (1) Each component of the process, system or subsystem is investigated to see if there are any possible failure modes; (2) Each failure mode's likely implications (failure impacts) are examined; (3) Occurrence, severity and detection for each discovered failure are assessed (Cicek and Celik, 2013). How frequently a certain failure cause is expected to occur is known as the occurrence (O). The evaluated severity of the failure's impact on the process, system and its surroundings are its severity (S). Detection (D) refers to the chance of the monitoring system(s) detecting a cause/mode of failure before the component/system is damaged and shut down (Pillay and Wang, 2003). According to Liu (2016), the traditional FMEA evaluates the O, S and D features using a 10-point linguistic scale. The greater the value, the more severe the attack, the higher the likelihood of a failure and the less the existing controls' ability to detect a failure (Haseeb et al., 2021). Detailed information about the ranking systems for each risk factor can be found in Liu (2016). Thereafter, for each failure mode, a risk priority number (RPN) is calculated to prioritise the failure modes. Pillay and Wang (2003) defined the RPN as

$$RPN = O \times S \times D \quad (1)$$

Failure modes are prioritised to choose effective preventative measures and control plans that may prevent the occurrence or mitigation of potential failures (Cicek and Celik, 2013; Liu, 2016).

3. Application

3.1. Voyage data recorder

The VDR is made of many components (see Figure 1) (Gallagher, 2015). These are standard for almost all manufacturers, unless they have additional functionality, such as remote access.

These components have many physical and digital interfaces, using internationally recognised formats such as Ethernet, USB, firewire, and IEC 61162 (i.e. Marine radio) to communicate with signal sources, download the stored data and run the data on an external computer (BS EN IEC 61162-1, 1996; BS EN IEC 61162-2, 1999).

3.2. Case study

The present study aims to uncover VDR cyber vulnerabilities, reveal which particular cyberattacks it is vulnerable to, and use the robust FMEA risk assessment to rank those risks.

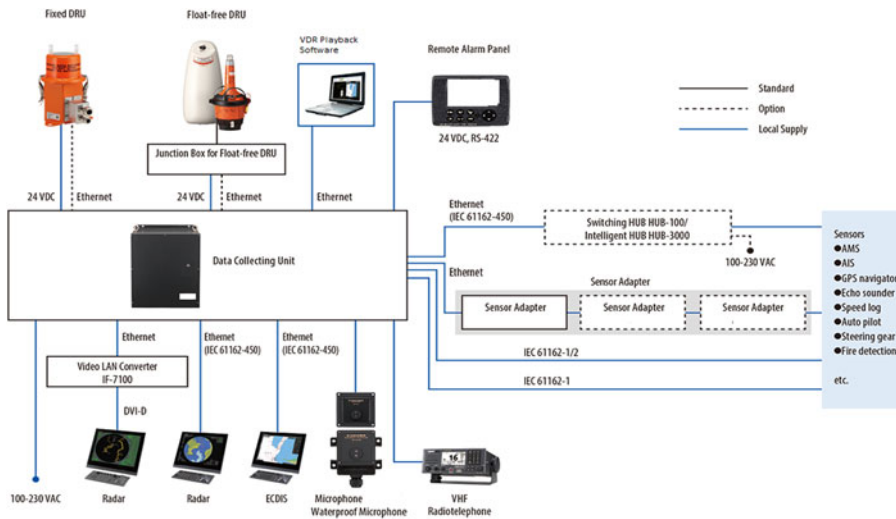


Figure 1. Configuration of VDR onboard (Gallagher, 2015).

3.2.1. Identification of cyber vulnerabilities and cyber-attacks for VDR

Since experts identify potential failure modes using FMEA methodology, participants with the appropriate experience were essential. Note, however, that reported cyber incidents for VDR are rare. Therefore, the initial data (cyber vulnerabilities and attacks) were collected from research papers (Silverajan et al., 2018; Kaleem Awan and Ghamdi, 2019; Tam and Jones, 2019; Jo et al., 2022; Tam et al., 2022) and accidents/incident reports (Kovacs, 2015; Santamarta, 2015). Then, potential failure modes were determined by experts based on cyber vulnerabilities derived from available publications. After that, the effects and causes of each failure mode were defined with the provided literature review. After the FMEA table was created in the framework of VDR cyber security, experts assigned scores in order to provide a data set for application of the FMEA process.

Four experts in maritime cybersecurity participated in this study. By considering selection of the experts, focus was on the relationship with maritime cyber security. Accordingly, an expert group, whose members are in a research laboratory with sectoral and academic functions in the field of maritime cyber security, were selected. The experts included one electronic engineer, two computer engineers and one maritime transportation engineer.

According to the VDR components in Figure 1, serial data (IEC 61162-1, IEC 61162-2), network data (IEC 61162-450), Modbus, and VHF and bridge audio data all have a number of inputs on the data acquisition /collection unit (DAU) (Danelec, 2021). It has also built-in UPS, and about 30 days of recording capacity on solid state drive (SSD). Some sensor data, such as heading, location and speed, are collected directly into the DAU through serial NMEA interfaces (IEC 61162), while other data (such as AIS, ECDIS and NAVTEX) are gathered over Ethernet into the DAU for serial National Marine Electronics Association (NMEA) sensors (Svilicic et al., 2019c). Protective fixed capsules and float-free capsules have Ethernet (100BASE-TX) and are powered from DAU with the power over Ethernet (PoE). The bridge control panel has an interface for operational performance test and is powered from USB or DAU PoE. Indoor and outdoor microphones have built-in amplifier, filters and a buzzer for self-test and are powered from DAU. VDR playback software (Windows-based application) provides real-time monitoring and data replay, and extracts data from the VDR through a web browser via Web Extractor tool. The technical infrastructure is summarised in Table 1.

The increase of usage of insecure network or serial data protocols (e.g. Modbus) in real-world systems dramatically increases risk. For this paper, this can introduce risks when devices (ECDIS, AIS, RADAR, sensors, etc.) send information to the VDR. Modbus is an open protocol that supports RS232/422/485 and Ethernet protocols, allowing communication between industrial devices, such as programmable

Table 1. *The technical specification of VDR components.*

DAU	Protective fixed capsule	Float-free capsule	Bridge control panel	Bridge microphone	VDR playback software
IEC 61162-1, IEC 61162-2 and Modbus for serial data	Ethernet interface	Ethernet interface	Ethernet interface	Powered from DAU (PoE)	Windows-based application
IEC 61162-450 for network data	Powered from DAU (PoE)	Powered from DAU (PoE)	Powered from DAU (PoE)		Extract VDR data from (web browser/web extractor tool)
SSD Inputs for bridge audio and VHF			USB connection		

logic controllers (PLCs), sensors and meters. Parian et al. (2020) stated that Modbus protocol has no confidentiality and data integrity, leaving it vulnerable to malware and man-in-the-middle attacks. Bhatia et al. (2014) and Queiroz et al. (2009) showed that Modbus protocol has vulnerabilities against flooding-based attacks and denial of service (DoS) attacks. Huitsing et al. (2008) defined 20 separate attacks for Modbus Serial, such as diagnostic register reset, remote start and slave reconnaissance. They categorised the impacts of the attacks against Modbus Serial in four groups: interception, interruption, fabrication and modification of target control system assets. The impacts of these attacks are loss of confidentiality, loss of control and loss of awareness.

The international standard series for application in marine navigation, radio communication and system integration (IEC 61162) can transmit serial and network data in the VDR, and while more secure than Modbus, still has vulnerabilities. NMEA 0183 is a standard which supports one-way serial data transmission from a single talker to multiple listeners (NMEA, 2021). Tran et al. (2021) stated that NMEA 0183 does not include any encryption, authentication or validation. Therefore, data are transmitted to VDRs (e.g. ship speed, position, depth) in printable ASCII characters (plaintext). Consequently, NMEA 0183 packets are vulnerable to DoS, spoofing and sniffing. Moreover, the RS-232 of serial interface family, which supports baud rate 4800 for NMEA 0183 using in the VDR, has vulnerability against buffer overflow attacks (Malviya, 2020). Previous research has shown that NMEA 0183 High Speed is similarly vulnerable (Amro, 2021).

NMEA 2000 controller area network (CAN) is a multi-transmitter/multi-receiver instrument network for interconnecting maritime electronic equipment that was launched after NMEA 0183. Despite being 50 times quicker than NMEA 0183, this standard is not designed to enable high-bandwidth applications, such as video (NMEA, 2021). NMEA 2000 shares vulnerabilities with its underlying CAN serial bus technology. Malicious code can be executed on sniffed packets in the broadcast and packets can be played back (replay attack), invalidate data or inject revised traffic (Amro, 2021). The replay attacks can be performed especially on the audio-visual system because of the insecure communication line between the cameras or microphone and receiving systems, such as VDR. Data can also be changed via replay attacks. This attack can be performed on a bridge microphone connected to a VDR, possible because of the lack of confidentiality and integrity security measures on CAN (Silverajan et al., 2018). These attacks, as well as DoS and trojan horses, could potentially reveal confidential data, create malfunctions, force system resets or even eliminate criminal evidence of industrial espionage and fraud (Kessler, 2021).

Ethernet (IEC 61162-450) is used for maritime systems, such as GPS, compass and AIS sensors, to transmit data to the VDR (Hemminghaus et al., 2021a). This protocol employs Ipv4 multicast with separate receiver groups dependent on the equipment type and is based on the UDP/IP stack (Hemminghaus et al., 2021a). On these networks, person-on-the-side (PotS) and person-in-the-middle (PitM) attacks are often possible, meaning an attacker can passively listen, or actively tamper or replay messages (Hemminghaus et al., 2021b). There is only one option for authentication, which is the message digest 5 (MD5) hash algorithm. However, the key of the MD5 hash can be broken easily (Hemminghaus et al., 2021b).

Web-based tools and software on a VDR can facilitate testing and servicing, retrieving stored data for playback and extracting data for safety and performance purposes. Common cyberattacks used against a web-based tool are SQL injection, XML injection and insecure serialisation. Attacks against VDR can use SQL keystroke injection, DDoS, ransomware, virus deployment, reverse shell access and obfuscation SSD corruption through USB drives on an integrated bridge system. Silverajan et al. (2018) also stated that some VDRs have been vulnerable to buffer overflows, flawed firmware update mechanisms and common injection vulnerabilities. Malicious payloads and harmful code, such as ransomware, malware, viruses and spyware, can be introduced with removable media, malicious firmware updates or a compromised device (e.g. sensor) in the connected system. Santamarta (2015) stated that there are vulnerabilities for the VR-3000 VDR that give attackers unauthorised remote network access to affected devices and execute arbitrary commands with root privileges. In this case, attackers can access, change or delete all recorded information in VDR. According to the VDR firmware update process for VR-3000, an attacker-controlled string could be executed if not properly sanitised. However, as they are not often

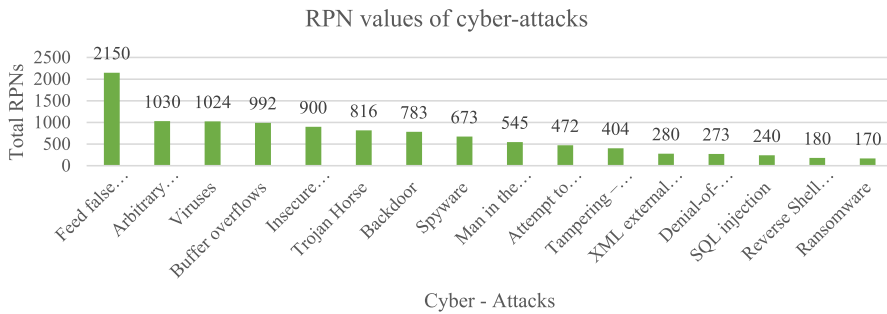


Figure 2. Cyber risk analysis for VDR.

sanitised, arbitrary commands with root privileges can be executed by remote unauthenticated attackers due to this vulnerability.

3.2.2. FMEA application and results

Supplied with the literature data mentioned, an expert group carried out the key FMEA procedures outlined in Section 2. After experts determined the potential failure modes based on cyber vulnerabilities derived from available publications, they consensually assigned an occurrence, severity and detectability ranking for each failure mode by using the 10-point linguistic scale. Lastly, Equation (1) was used for the calculation of the RPN values, and all performed actions displayed in Table 2 are referred to as the FMEA analysis worksheet.

The quantitative findings of FMEA application to cyber risk assessment are highlighted to clarify, prioritise and develop the essential preventive measures. At this point, special attention should be paid to the RPN values of the cyberattacks (failure mode) and VDR components (failed components) in order to reveal the significant cyberattacks and vulnerabilities specifically to the VDR. Thus, the RPN values of cyberattacks are shown in Figure 2 to highlight the most significant cyberattacks on the VDR. Accordingly, the top three serious cyberattacks for VDR are feeding false information, command injection and viruses.

On the other hand, Figure 3 demonstrates the RPN values of VDR components in order to expose the most critical failed components. According to the results, the most vulnerable VDR components are DAU, connect and remote access playback software, and bridge control panel.

Beyond that, further in-depth analysis is also possible. For example, investigating cyberattacks on each component may also assist in developing satisfactory precautions and improving VDR cybersecurity.

Figure 4 depicts the RPN values of cyberattacks that are especially relevant to the DAU. Accordingly, the most dangerous attack for DAU is to feed fake information into the VDR with 540 RPN values. Considering the average value of the RPN value of DAU (243), arbitrary command injection with root privileges, buffer overflows, backdoor and viruses are among other crucial cyberattacks that jeopardise the cybersecurity of DAU. Control measures for the prioritised failure modes is discussed in detail in the next subsection to clarify the implementation of the FMEA application results in cyber risk assessment on VDR.

3.2.3. Findings and discussions

According to the overall results, feeding false information into the VDR is the most critical cyberattacks for a VDR. Because an attack can be carried out on every part of the VDR because the VDR generally has high-level occurrence, severity and low-level detectability for all its parts. Essentially, it is not directly a specific cyberattack against VDR, but is indirect attack which caused by cyberattacks targeted other bridge onboard systems. False information can be delivered to the VDR by cyberattacks against any bridge integrated systems that send the data to VDR, such as unauthorised remote access to ECDIS, GPS spoofing or AIS spoofing. These attacks vary according to the vulnerability of each vessel's own

Table 2. FMEA analysis worksheet.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
DAU	Man in the middle attack	<ul style="list-style-type: none"> To be able to bypass IP address authentication ARP spoofing utility that scans the target's network for IP and MAC addresses Insecure communication protocols 	<ul style="list-style-type: none"> Eavesdrop or to impersonate one of the parties, gain full visibility any online data exchange, alter the packets, and steal data via IP spoofing, DNS spoofing (for web-based VDR connect and RAS), and ARP spoofing (for DAU and fixed and float capsules) 	5	6	8	240
Protective fixed and float-free capsules				2	4	10	80
Web-based VDR connect and remote access solution				5	9	5	225
DAU	Arbitrary command injection with root privileges	<ul style="list-style-type: none"> Insufficient input validation 	<ul style="list-style-type: none"> Remote access to the database, full control of data, such as delete and modify data Remote access to folders, directories, files, etc. 	5	10	9	450
Protective fixed and float-free capsules				2	8	10	160
Bridge control panel				6	10	7	420
Web-based VDR connect and remote access solution	SQL injection	<ul style="list-style-type: none"> Older functional interfaces and non-validated input vulnerabilities in a database 	<ul style="list-style-type: none"> Unauthorised viewing of recorded data, delete, change, destroy of data within database (MySQL) 	4	10	6	240

Table 2. continued.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
Web-based connect and remote access solution	VDR Insecure serialisation	<ul style="list-style-type: none"> Unsafe programming language high level languages such as Python c# browser interface code (html java) and deserialisation function 	<ul style="list-style-type: none"> Modifying the serialised object to obtain admin privileges and tamper with the data 	10	10	9	900
Web-based connect and remote access solution	VDR XML external entity injection (XXE)	<ul style="list-style-type: none"> A weakly configured XML parser 	<ul style="list-style-type: none"> Exposure of sensitive data, server-side request forgery (SSRF), or denial of service attacks 	7	8	5	280
DAU	Ransomware	<ul style="list-style-type: none"> Visiting a malicious or hacked website or clicking on a dangerous link in a spam e-mail Human factor by bridge control panel via USB stick or internet/Ethernet connection 	<ul style="list-style-type: none"> Lock the system without damaging any files by using a technique called crypto viral extortion. Encrypting the victim's files and making them inaccessible 	8	10	1	80
Protective fixed and float-free capsules				2	9	3	54
Bridge microphones				2	2	1	4
Bridge control panel				4	8	1	32
DAU	Backdoor	<ul style="list-style-type: none"> Default or weak passwords Human factor by bridge control panel via USB stick or internet/Ethernet connection 	<ul style="list-style-type: none"> Record your keyboard input, Copy critical data from computer storage, Abusing the microphone and camera to spy on others. 	4	9	9	324

Table 2. continued.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
Protective fixed and float-free capsules				3	3	8	72
Bridge microphones				3	5	9	135
Bridge control panel				4	7	9	252
DAU	Viruses	<ul style="list-style-type: none"> Clicking on a malicious link in a spam e-mail or visiting a malicious or compromised website Human factor by bridge control panel via USB stick or internet/Ethernet connection 	<ul style="list-style-type: none"> Slow system speed Errors in computing behaviour Unknown data loss Repeated computer crashes Spread from one platform to the next Damage or steal data from a device 	8	9	4	288
Protective fixed and float-free capsules				5	8	8	320
Bridge microphones				4	5	8	160
Bridge control panel				8	8	4	256
DAU	Spyware	<ul style="list-style-type: none"> Downloading bundle ware, or bundled software packages Visiting a compromised website or opening a malicious attachment in an email. Human factor by bridge control panel via USB stick or internet/Ethernet connection 	<ul style="list-style-type: none"> Data theft and identity fraud Computer damages 	4	7	5	140
Protective fixed and float-free capsules				1	1	8	8
Bridge microphones				6	7	9	378

Table 2. continued.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
Bridge control panel DAU	Trojan Horse	<ul style="list-style-type: none"> • Malware that is sent to the user's device as an attachment in an email or as a free-to-download file. • Human factor by bridge control panel via USB stick or internet/Ethernet connection 	<ul style="list-style-type: none"> • Data deletion, data blocking, data modification, and data copying • Leading computer or network functionality to be disrupted 	3	7	7	147
				4	7	7	196
Protective fixed and float-free capsules				3	10	8	240
Bridge microphones				2	5	10	100
Bridge control panel				5	8	7	280
DAU	Tampering –replay attack	<ul style="list-style-type: none"> • Malwares, such as Trojan, ransomware, backdoor • ARP spoofing 	<ul style="list-style-type: none"> • Data deletion, data blocking, data modification, and data copying 	2	5	9	90
Protective fixed and float-free capsules				3	10	8	240
Bridge microphones				1	2	10	20
Bridge control panel				2	3	9	54
DAU	Denial-of-Service (DoS)	<ul style="list-style-type: none"> • A DoS attack is carried out by flooding the targeted host or network with traffic until it becomes inaccessible or fails, denying legitimate users access. 	<ul style="list-style-type: none"> • Extremely poor network performance (opening files or accessing websites), • Inability to visit any website or the unavailability of a certain website. 	5	8	1	40
Protective fixed and float-free capsules				1	2	1	2

Table 2. continued.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
Bridge microphones				7	8	3	168
Bridge control panel				7	9	1	63
DAU	Reverse shell access	<ul style="list-style-type: none"> • A remote command execution vulnerability 	<ul style="list-style-type: none"> • Remote access all the system 	2	9	10	180
DAU	Buffer overflows	<ul style="list-style-type: none"> • When a software tries to put more data in a buffer than it can contain, or when it tries to place data in a memory location beyond the buffer, a buffer overflow problem occurs. 	<ul style="list-style-type: none"> • Cause the execution of malicious code 	6	8	9	432
Web-based VDR connect and remote access solution				7	10	8	560
DAU	Feed false information into the VDR	<ul style="list-style-type: none"> • GPS, AIS spoofing, • Attacks to ECDIS, RADAR 	<ul style="list-style-type: none"> • Saving inaccurate data to VDR • Misleading investigators during an accident investigation 	6	10	9	540
Protective fixed and float-free capsules				6	10	9	540
Bridge microphones				2	5	9	90
Bridge control panel				6	10	7	420
Web-based VDR connect and remote access solution				8	10	7	560

Table 2. continued.

Failed component	Failure mode	Failure causes	Failure effect	Occurrence	Severity	Detectability	RPN
DAU	Attempt to access other ship systems through the connections to the VDR	<ul style="list-style-type: none"> • An attacker may try to send malware to the other systems by introducing it into the VDR so that it disseminates through the data links to the connected equipment. 	<ul style="list-style-type: none"> • GPS, AIS spoofing, • Attacks to ECDIS, RADAR • Critical ship accidents such as grounding, collision, sinking • Saving inaccurate data to VDR • Misleading investigators during an accident investigation 	2	8	10	160
Protective fixed and float-free capsules				1	8	10	80
Bridge microphones				1	8	9	72
Bridge control panel				2	8	10	160

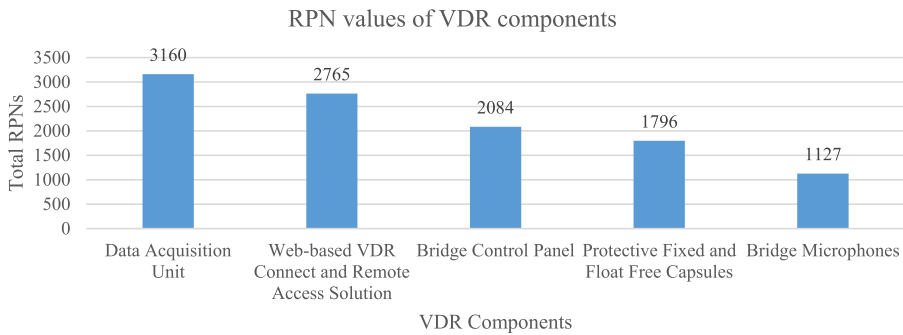


Figure 3. Cyber risk analysis for VDR components.

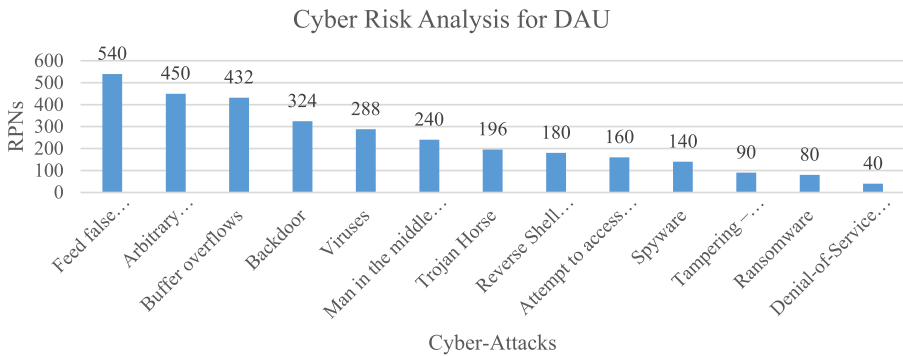


Figure 4. Cyber risk analysis for DAU.

technical infrastructure and may result in the out-of-service of each device, changing the information it contains, and infiltration of other integrated systems. For instance, ECDIS charts and routes can be deleted or modified. If a VDR stores that false data, it would provide false information to accident investigators. Further research of attacks on other systems to feed false information the VDR, and mitigations thereof, is out of the scope of this paper.

On the other hand, arbitrary command injection attacks have the second highest RPN. Such attacks can be carried out as one of the most critical attacks on the DAU, as one of the medium level risks on the capsules, and as the riskiest attack on the bridge control panel. This arises from the weaknesses of an unprotected system which enables the execution of arbitrary commands. During arbitrary command injections, an attacker could get full control of the host operating system or the server, compromising the software and all its data, which is high impact.

Viruses, which have a relatively high RPN, are also regarded as serious cyber risks. There are several types of malwares that affect the DAU, protective fixed and float-free capsules, bridge control panel and bridge microphones. The riskiest ones are those that can delete and steal VDR data, flood VDR networks, and slow down system performance. Spyware, more specifically, is the riskiest for the bridge microphone. This could inform the counterparty in the accident. Ways to prevent malware from tampering, stealing and deleting VDR data is to set up secure backup systems for storage, and more secure networks for data transfers.

In the case of buffer overflow attack, attackers can overwrite memory and change the execution path. For this reason, VDRs with remote access have a higher risk against this attack. Although insecure serialisation is not risky for VDRs overall, it has the highest RPN value (900) when evaluated separately. Furthermore, it is the riskiest cyberattacks for web-based VDR connect and remote access solution and VDR playback software. If serialisation of data goes wrong, information can be lost as objects are deconstructed. Conversely, if deserialisation is not secure, unauthorised users can input malicious code,

providing an entry point for the attacker and increasing the attack surface. An attacker might alter serialised objects to transfer malicious data into the software application code, for example, if a website erroneously deserialises data. Digital signatures or other integrity control methods can be introduced to prevent this kind of malicious object creation or other data interference. User privileges can also follow least privilege principal.

Although this paper focuses on the attacks that have been ranked with higher-than-average risks using FMEA, it should not be forgotten that attacks below the average risk and but with high-level effects should also be taken into consideration. Furthermore, when the results of this study are evaluated from a different viewpoint, it is seen that the most vulnerable components of VDR is the DAU. Because it has a numerous protocols and standard interfaces for serial and network data, operating system, network and Ethernet connections. It has more integration of information and private industrial control system technologies. Therefore, it has more several vulnerable entrances point for the attackers, as mentioned in Section 4.2.1 in comparing with other parts of VDR. Moreover, DAU, which is the main and compulsory component of VDR, is the first and the most important place for collecting the data and the data stay on it for the longest time. For this reason, when any one of the assessed attacks is actualised against DAU, the expected impact of it is also high.

The second more risky component of VDR is connect and remote access solution and playback software. It is a web-based solution and the data playback on the VDR software in a PC in real time. The connect and remote access solution that is optional products for VDR transmits the data from the VDR via satellite to the home office. In this context, it has information technologies and software functions instead of industrial control system technologies. Since the vulnerabilities for web-based networking or authorised access exist more and attackers are familiar to perform cyberattacks against information technologies, especially against web-based applications, this part of VDR is resulted as critically risky.

Ranked three for critical risks according to this study is the bridge control panel. This is a console which has an interface with the VDR to carry out operational performance test regularly, shows any kind of system errors with alert functions, has buttons to stop or start recording, has USB stick entrance, and is powered by DAU. The possibilities and detectability of the cyberattacks against bridge control panels are in the medium level, due to the smaller number of entrances point, such as having only Ethernet interface with DAU. Cyberattacks can exploit the Ethernet vulnerabilities, be leaked from DAU and be caused by human operation on console intentionally or unintentionally.

The protective fixed and float-free capsules and bridge microphones are in the last order in terms of cyber risk assessment for VDR. Because they are more physical equipment instead of being hardware, software, information or control systems. The protective fixed and float-free capsules have Ethernet interface with DAU, such as on a bridge control panel. They are only used for reaching last 48 h data in case of any accident. Basically, the possibility of cyberattacks against capsules are less than against a bridge control panel due to not having user function, excluding Ethernet vulnerabilities and leakage from DAU. Bridge microphones have the least risk according to this study. They do not retain data; therefore, the most severe consequence of the cyberattacks against bridge microphones can be denial of service, break of the bridge conversation and VHF communication instead of cyberattacks targeting data.

4. Conclusion

Although great efforts have been made to improve cybersecurity onboard ships IT and OT systems, cyberattacks cannot entirely prevented for VDR because of the nature of the cyber world. However, the effects of intentional or unintentional actions can be reduced by conducting a cyber risk assessment to develop effective control measures that enable safeguarding VDR from current and emerging cybersecurity threats. Therefore, a cybersecurity risk assessment of VDR has been conducted in order to identify failure components, cyber vulnerabilities and potential cyberattacks to develop feasible measures via the FMEA method.

According to the FMEA results, a serious level of preventive action is required especially for certain cyberattacks, such as feeding false information, command injection, and viruses and VDR components

(DAU, remote access, playback software, etc.). These attacks vary depending on the vulnerabilities of each ship's specific technological architecture and can result in the device being taken out of service, the information it carries being changed, and other interconnected systems being infiltrated. Furthermore, those attacks may lead the VDR to receive faulty data, which is then recorded in the VDR's body, giving accident investigators misleading information. In addition, the DAU is the most critical component in terms of having several interfaces for serial and network data, an Ethernet connection, and collecting all vital information in its own body for a long time. In this respect, VDR should be designed by taking into consideration specially built-in library functions instead of calling OS commands directly, and a white list for inputs to ensure the system allows solely pre-approved inputs, secure application programming interfaces (APIs), antivirus, and anti-spam programs in the OS used in DAU, principles of least privilege and network segmentation for all components of VDR, and network traffic monitoring connected to VDR.

Given that these cyberattacks against VDR have impacted a large number of shareholders in the shipping industry (shipowners/operators, accident investigators, P&I Clubs, etc.), minimising the cyber vulnerability and preventing the risk of cyberattacks is crucial. Thus, preventive and control measures have been considered to improve the cybersecurity of VDR. Consequently, this study makes valuable contributions to improving ships' safety management systems, especially from a cybersecurity perspective through proposing mitigation, and recovery in the case of the identified attacks, and determining vulnerable components of the VDR. Moreover, by considering the elements of the usage of the data from VDR and its network connectivity for the future adoption of digital twins for ships, which basically are a mirror of this same data, the cyberattacks against VDR can be handled early and undesirable outcomes can be prevented by monitoring at early stage, because the digital twin of a ship embodies simulation and all data procurable during the entire lifetime of the ship. Therefore, the infinite number of process with the digital twin of a ship, such as the prevention of costly failures on VDR due to the cyberattacks, the enhancement of strategic technology trends for cyber security, and a glimpse into what can happen as a cyberattack against VDR now and far into the future, can be carried out by using advanced analytical, monitoring and predictive capabilities, test processes and services.

Acknowledgment. The authors would like to thank the experts for their assessment, comments, and efforts towards improving our manuscript.

Funding statement. This study is partially funded by The Scientific and Technological Research Council of Turkey (TÜBİTAK) - 2214-A – International Research Fellowship Programme for PhD Students [REF: 53325897-115.02-152823]. This study is also supported by University of Plymouth, Cyber-SHIP Lab.

References

- ABS (American Bureau of Shipping).** (2016). *The Application of Cybersecurity Principles To Marine and Offshore Operations*. ABS Cybersafety Volume 1. Spring, TX 77389 USA.
- Akula, S. K. and Salehfar, H.** (2021). Risk-based Classical Failure Mode and Effect Analysis (FMEA) of Microgrid Cyber-Physical Energy Systems. In *2021 North American Power Symposium (NAPS)*. IEEE 1–6.
- Amro, A.** (2021). Cyber-Physical tracking of IoT Devices: A Maritime Use Case. In *Norsk IKT-Konferanse for Forskning Og Utanning*, Vol. 3.
- Babineau, G. L., Jones, R. A. and Horowitz, B.** (2012). A System-Aware Cybersecurity Method for Shipboard Control Systems with A Method Described to Evaluate Cybersecurity Solutions. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 99–104.
- Barkow, I., Leopold, T., Raab, M., Schiller, D., Wenzig, K., Blossfeld, H. P. and Rittberger, M.** (2011). 20 RemoteNEPS: data dissemination in a collaborative workspace. *Zeitschrift für Erziehungswissenschaft*, **14**(2), 315–325.
- Bhatia, S., Kush, N., Djamaludin, C., Akande, J. and Foo, E.** (2014). Practical Modbus flooding attack and detection. *Conferences in Research and Practice in Information Technology Series*, **149**, 57–65.
- BIMCO.** (2020). *The Guidelines on Cyber Security onboard Ships - Version 4*. BIMCO: Copenhagen, Denmark.
- Bolbot, V., Theotokatos, G., Boulougouris, E. and Vassalos, D.** (2020). A novel cyber-risk assessment method for ship systems. *Safety Science*, **131**, 104908.
- Cicek, K. and Celik, M.** (2013). Application of failure modes and effects analysis to main engine crankcase explosion failure on-board ship. *Safety Science*, **51**(1), 6–10.

- Danelec.** (2021). DM100 VDR, Voyage Data Recorder. VDR Manufacturer Brochure. <https://denmark.xcontain.com/company/danelec-electronics-a-s/>
- Danelec Systems.** (2016). White Paper on Vdr Cybersecurity.
- Gallagher, S.** (2015). Hacked at sea: Researchers find ships' data recorders vulnerable to attack. *ArsTECHNICA*. <https://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-records-vulnerable-to-attack/>
- Glomsrud, J. A. and Xie, J.** (2019). A Structured STPA Safety and Security Co-Analysis Framework for Autonomous Ships. In *European Safety and Reliability Conference*, Germany, Hannover.
- Gunes, B., Kayisoglu, G. and Bolat, P.** (2021). Cybersecurity risk assessment for seaports: A case study of a container port. *Computers & Security*, **103**, 102196.
- Guzman, N. C., Kufalor, D. K. M., Kozine, I. and Lundteigen, M. A.** (2019). Combined Safety and Security Risk Analysis Using the UFoI-E Method: A Case Study of an Autonomous Surface Vessel. In *Proceedings of the 29th European Safety and Reliability Conference*, Lower Saxony, Germany, 22–26.
- Haseeb, J., Mansoori, M. and Welch, I.** (2021). Failure Modes and Effects Analysis (FMEA) of Honey-pot-Based Cybersecurity Experiment for IoT. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 645–648.
- Heering, D., Maennel, O. M. and Venables, A. N.** (2021). Shortcomings in Cybersecurity Education for Seafarers. In *Developments in Maritime Technology and Engineering*, 49–61. CRC Press.
- Hemminghaus, C., Bauer, J. and Padilla, E.** (2021a). BRAT: A BRidge attack tool for cybersecurity assessments of maritime systems. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, **15**(1), 35–44. doi:10.12716/1001.15.01.02
- Hemminghaus, C., Bauer, J. and Wolsing, K.** (2021b). SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems Using Digital Signatures. *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. doi:10.1109/ISNCC52172.2021.9615738
- Huitsing, P., Chandia, R., Papa, M. and Sheno, S.** (2008). Attack taxonomies for the modbus protocols. *International Journal of Critical Infrastructure Protection*, **1**(C), 37–44. doi:10.1016/j.ijcip.2008.08.003
- IMO.** (2012). Adoption of Revised Performance Standards for Shipborne Voyage Data Recorders (VDRs). IMO Resolution MSC 333(90).
- IMO (International Maritime Organization).** (2016). Guidelines On Maritime Cyber Risk Management. IMO MSC-FAL.1/Circ.3.
- Jo, Y., Choi, O., You, J., Cha, Y. and Lee, D. H.** (2022). Cyberattack models for ship equipment based on the MITRE ATT&CK framework. *Sensors*, **22**(5), 1860. doi:10.3390/s22051860
- Kaleem Awan, M. S. and Ghamdi, M. A. A.** (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*, **7**(10), doi:10.3390/jmse7100350
- Katsikas, S. K.** (2017). Cybersecurity of the Autonomous Ship. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, pp. 55–56.
- Kavallieratos, G. and Katsikas, S.** (2020). Managing cybersecurity risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*, **8**(10), 768.
- Kavallieratos, G., Katsikas, S. and Gkioulos, V.** (2018). Cyberattacks against the autonomous ship. In *International Workshop on Security and Privacy Requirements Engineering, International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems*, Cham: Springer, 20–36.
- Kessler, G. C.** (2021). The can bus in the maritime environment – technical overview and cybersecurity vulnerabilities. *TransNav*, **15**(3), 531–540. doi:10.12716/1001.15.03.05
- Kim, M., Jung, T. H., Jeong, B. and Park, H. S.** (2020). Autonomous shipping and its impact on regulations, technologies, and industries. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, **4**(2), 17–25.
- King, J.** (2005). The security of merchant shipping. *Marine Policy*, **29**(3), 235–245.
- Kovacs, E.** (2015). Ship Data Recorders Vulnerable to Hacker Attacks. SecurityWeek. <https://www.securityweek.com/ship-data-recorders-vulnerable-hacker-attacks>
- Liu, H. C.** (2016). FMEA using uncertainty theories and MCDM methods. In *FMEA Using Uncertainty Theories and MCDM Methods*. Singapore: Springer, 13–27, doi:10.1007/978-981-10-1466-6.
- Liu, H. C., You, J. X., Ding, X. F. and Su, Q.** (2015). Improving risk evaluation in FMEA with a hybrid multiple criteria decision-making method. *International Journal of Quality & Reliability Management*, **32**(7), 763–782. doi:10.1108/IJQRM-10-2013-0169
- Malviya, N.** (2020). RS-232 and RS-485. Infosec. <https://resources.infosecinstitute.com/topic/rs-232-and-rs-485/>
- MD (Marine Digital).** (2022). Cybersecurity in shipping and port technologies: examples of cyber-attacks in maritime. Retrieved: 15.03.2022. From: https://marine-digital.com/cybersecurity_in_shipping_and_ports
- Meland, P. H., Bernsmed, K., Wille, E., Rødseth, ØJ and Nesheim, D. A.** (2021). A retrospective analysis of maritime cybersecurity incidents. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, **15**(3), 519–530.
- NMEA.** (2021). NMEA Standards. National Marine Electronics Association. https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard
- OCIMF (Oil Companies International Marine Forum).** (2020). Recommendations on the Proactive Use of Voyage Data Recorder Information. (Revised edition 2020). London, UK.

- Omitola, T., Downes, J., Wills, G., Zwolinski, M. and Butler, M. (2018). Securing Navigation of Unmanned Maritime Systems. *Proceedings of the International Robotic Sailing Conference 2018*, Southampton, United Kingdom, 31-08-2018.
- Papastergiou, S., Polemi, N. and Karantjias, A. (2015). CYSM: AN Innovative Physical/Cybersecurity Management System for Ports. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham, pp. 219–230.
- Parian, C., Guldemann, T. and Bhatia, S. (2020). Fooling the master: Exploiting weaknesses in the modbus protocol. *Procedia Computer Science*, **171**(2019), 2453–2458. doi:10.1016/j.procs.2020.04.265
- Perera, L. P. and Mo, B. (2020). Ship performance and navigation information under high-dimensional digital models. *Journal of Marine Science and Technology*, **25**(1), 81–92.
- Piccinelli, M. and Gubian, P. (2013). Modern ships Voyage Data Recorders: A forensics perspective on the Costa Concordia shipwreck. *Digital investigation*, **10**, S41–S49.
- Pillay, A. and Wang, J. (2003). Modified failure mode and effects analysis using approximate reasoning. *Reliability Engineering & System Safety*, **79**(1), 69–85.
- Queiroz, C., Mahmood, A., Hu, J., Tari, Z. and Yu, X. (2009). Building A SCADA Security Testbed. *NSS 2009 - Network and System Security*, 357–364. doi:10.1109/NSS.2009.82
- Ralston, P. A., Graham, J. H. and Hieb, J. L. (2007). Cybersecurity risk assessment for SCADA and DCS networks. *ISA Transactions*, **46**(4), 583–594.
- Santamarta, R. (2015). Maritime security: Hacking into a voyage data recorder (VDR). IOActive.
- Shang, W., Gong, T., Chen, C., Hou, J. and Zeng, P. (2019). Information security risk assessment method for ship control system based on fuzzy sets and attack trees. *Security and Communication Networks*, **2019**, Article ID 3574675, 11 pages. <https://doi.org/10.1155/2019/3574675>
- Silverajan, B., Ocak, M. and Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, IThings/Gree*, 15–20. doi:10.1109/Cybermatics_2018.2018.00037
- Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA From Theory to Execution*. Milwaukee, Wisconsin: Quality Press.
- Svilicic, B., Kamahara, J., Celic, J. and Bolmsten, J. (2019a). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, **18**(3), 509–520.
- Svilicic, B., Rudan, I., Frančić, V. and Doričić, M. (2019b). Shipboard ECDIS cybersecurity: Third-party component threats. *Pomorstvo*, **33**(2), 176–180. doi:10.31217/p.33.2.7
- Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. (2019c). Maritime cyber risk management: An experimental ship assessment. *The Journal of Navigation*, **72**(5), 1108–1120.
- Tam, K. and Jones, K. (2018). Cyber-risk Assessment for Autonomous Ships. In *2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity)*. IEEE, pp. 1–8.
- Tam, K. and Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, **18**(1), 129–163. doi:10.1007/s13437-019-00162-2
- Tam, K., Moara-Nkwe, K. and Jones, K. (2021). A Conceptual Cyber-Risk Assessment of Port Infrastructure. *2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs*. 28-29 January 2021, Virtual Conference, Paredes, Portugal.
- Tam, K., Hopcraft, R., Moara-Nkwe, K., Misa, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T. and Jones, K. (2022). Case study of a cyber-physical attack affecting port and ship operational safety. *Journal of Transportation Technologies*, **12**(01), 1–27. doi:10.4236/jtts.2022.121001
- Tran, K., Keene, S., Fretheim, E. and Tsikerdekis, M. (2021). Marine network protocols and security risks. *Journal of Cybersecurity and Privacy*, **1**(2), 239–251. doi:10.3390/jcp1020013
- Zhou, X. Y., Liu, Z. J., Wang, F. W., Wu, Z. L. and Cui, R. D. (2020). Towards applicability evaluation of hazard analysis methods for autonomous ships. *Ocean Engineering*, **214**, 107773.
- Zhou, X. Y., Liu, Z. J., Wang, F. W. and Wu, Z. L. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Engineering*, **222**, 108569.